(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 January 2002 (24.01.2002)

PCT

(10) International Publication Number
WO 02/06971 A1

(51) International Patent Classification[7]: G06F 15/173

(21) International Application Number: PCT/US01/22107

(22) International Filing Date: 13 July 2001 (13.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/217,968 13 July 2000 (13.07.2000) US

(71) Applicant *(for all designated States except US)*: **APRISMA MANAGEMENT TECHNOLOGIES, INC.** [US/US]; 121 Technology Drive, Durham, NH 03824 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **LEWIS, Lundy, M.** [US/US]; 480 Greenville Road, Mason, NH 03048 (US).

(74) Agent: **HENDERSON, Norma, E.**; 13 Jefferson Drive, Londonderry, New Hampshire 03053 (US).

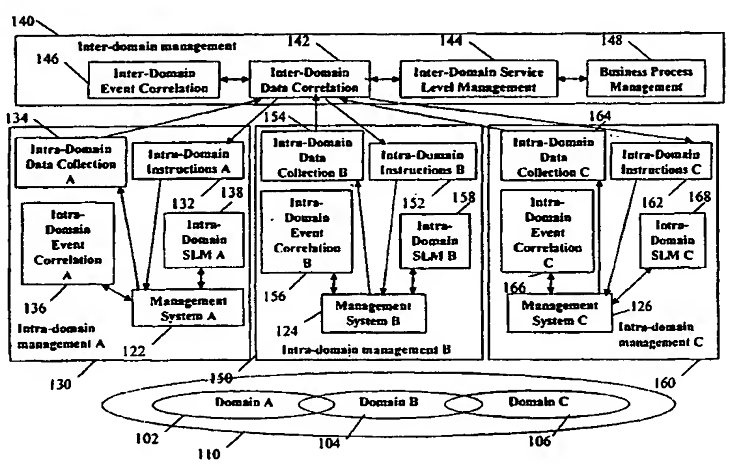
(81) Designated States *(national)*: AU, CA, US.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND APPARATUS FOR A COMPREHENSIVE NETWORK MANAGEMENT SYSTEM



(57) Abstract: In a system for managing data, voice, application and video networks and associated systems and services that comprise multiple, interconnected network technologies, a management system (130, 150, 160) suited for a particular networking technology manages each separate domain (110). Multiple managemnt systems thus mana ge multiple domains with respect to faults, configuration, accounting, performance, and security management. The management systems that manage the individual networking technology domains are then managed by a higher-level system, called an inter-domain management system (140), which performs cross-domain management. The individual management systems of the invention collect data from their respective domains and provide it to an intra-domain data collection function (134, 154, 164). This data is then utilized by an inter-domain data correlation function (142) to determine what instruction should be sent from anintra-domain instruction function (132, 152, 162) to each management system for implementation in its respective technology domains.

WO 02/06971 A1

Method and Apparatus for a Comprehensive Network Management System
(20002/10004 | HEN-10004)

Related Applications

This application claims priority to United States Provisional Application Ser. No. 60/217,968, filed July 13, 2000.

Field of the invention

The invention relates to management of communications networks and, in particular, to comprehensive management of a network comprised of multiple interconnected networking technologies and associated systems, including management of multi-domain services.

Background

Traditionally, networks and services that consist of, or depend upon, several different interconnected networking technologies and associated systems and applications, often referred to as multi-domain or heterogeneous networks, have been managed piece-meal, typically utilizing several management systems dedicated to the specific networking technologies and applications. This makes it very difficult to manage the multi-domain network from an end-to-end perspective. Because this method is non-comprehensive and largely non-automated, it tends to be expensive and error-prone, requiring the coordination and use of many different individuals and resources, as well as disparate management systems.

Today's business and service networks are complex. Since the current state of any particular network has more than likely evolved in a piecemeal fashion, it likely includes heterogeneous kinds of network technologies, equipment from multiple vendors, and various kinds of management methods. To make matters worse, management methods vary between countries and even between districts within countries. In many cases, the result is either

piecemeal management, in which narrowly focused management solutions co-exist but do not cooperate, or no management at all.

FCAPS (fault, configuration, accounting, performance, and security) management is possible for most individual networking technologies and associated systems and applications. However, these functions are typically provided by management systems that manage only that specific kind of networking technology, system, or application. Aprisma Management Technologies' Spectrum® Management System is an example of an existing management system that has this capability. The best case, however, would be integrated management, in which these management techniques cooperate in a standardized management framework.

What has been needed, therefore, is a consolidated, automated management tool that can manage networks and services that extend across multiple interconnected underlying networking technologies and associated systems and applications, thus providing management for multi-domain services.

Objects of the invention

The object of the present invention is to provide a means by which to manage a multi-domain network consisting of multiple interconnected networking technologies and associated systems and applications, including the ability to perform fault, configuration, accounting, performance, and security (FCAPS) management. A further object of the present invention is to provide end-to-end management of multi-domain services, including element, network, service, and business process management.

Summary

The comprehensive network management system of the invention (i) integrates the management of networks, systems, business applications, and services (ii) integrates the areas of fault, configuration, accounting, performance, and security management, (iii) integrates the element, network,

service, and business layers of management information, (iv) integrates the management of diverse networking technologies, and (v) integrates the management methods of both telecommunications and data communications networks.

The invention is a comprehensive system for managing data, voice, application and video networks and associated systems and services that comprise multiple, interconnected network technologies. In one aspect of the invention, a management system suited for a particular networking technology manages each separate technology domain. Multiple management systems thus manage multiple domains with respect to fault, configuration, accounting, performance, and security (FCAPS) management. The management systems that manage the individual networking technology domains are then themselves managed by a higher-level system, called an inter-domain management system, which performs the task of cross-domain management.

The individual management systems of the invention collect data from their respective technology domains and provide it to an intra-domain data collection function. This data is then utilized by an inter-domain data correlation function to determine what instructions should be sent from an intra-domain instruction function to each management system for implementation in its respective technology domain. The comprehensive management system thus collects data from each lower-level management system and, if required, sends operational instructions back to each lower level system.

In the present invention, management functions are performed from a single console and over multiple interconnected underlying networking technologies. The enabling technology for cross-domain management is the same technology that permits operation, administration and maintenance of the underlying networking technologies. Event correlation and service level management are performed at both the intra-domain and inter-domain levels, and business process management is performed at the inter-domain level.

Brief Description of the Drawings

Fig. 1 is a high-level block diagram of an embodiment of a comprehensive network management system according to the present invention;

Fig. 2 is a table illustrating the different dimensions of integrated network management;

Fig. 3 is a block diagram illustrating the generic components of a network;

Fig. 4 illustrates two different conceptual models for the integration of element and network management;

Fig. 5 is a block diagram illustrating the conceptual architecture of an enterprise management system that may be employed for cross-domain management in an embodiment of the invention;

Fig. 6 is an example of a network comprised of multiple interconnected networking technologies that may be managed by use of the present invention;

Fig. 7 is utilized to discuss the management challenge provided by the management of domains controlled by different entities;

Fig. 8 is a conceptual model of intra-domain event correlation as utilized by the present invention;

Fig. 9 is the Telecommunications Model Network (TMN) conceptual model of integrated management;

Fig. 10 is a conceptual depiction of how service level management is utilized in conjunction with enterprise management in one embodiment of the invention; and

Fig. 11 illustrates the operation of an embodiment of the comprehensive network management system of the present invention.

Detailed Description

The present invention is a comprehensive network management system for managing data, voice, application and video networks that (i) integrates the management of diverse, but connected network technologies, (ii) includes the

management of systems and software applications at customer premises, and (iii) allows for the provisioning, billing, and control of services that span across multiple kinds of networks. The invention allows comprehensive network management from a single console and over multiple interconnected underlying networking technologies and multi-domain services. It is an automated, consolidated management tool. It has tight integration with underlying element and network management systems.

In the present invention, a management system suited for a particular networking technology (e.g. optical networks, ATM networks, LANS, types of computer systems, types of software applications, etc) manages each separate technology domain within a multi-domain network with respect to fault, configuration, accounting, performance, and security (FCAPS) management. A higher-level system, called a comprehensive management system, performs the task of managing the individual management systems. This comprehensive system collects data from the multiple lower-level management systems and, if required, sends operational instructions to each lower-level management system.

Among other advantages, the invention enables end-to-end FCAPS management, element/network/service/business management, and service provisioning and monitoring from a single console over multiple interconnected networking technologies. Important features of the comprehensive management system of the invention include: (i) domain-specific event correlation, (ii) network, systems, and application management, (iii) layered Telecommunications Model Network (TMN)-style management, and (iv) FCAPS-style management.

The comprehensive network management system of the invention (i) integrates the management of networks, systems, business applications, and services (ii) integrates the areas of fault, configuration, accounting, performance, and security management, (iii) integrates the element, network, service, and business layers of management information, (iv) integrates the management of diverse networking technologies, and (v) integrates the

management methods of both telecommunications and data communications networks.

Fig. 1 is a high-level block diagram of an implementation of an embodiment of a comprehensive network management system according to the present invention. Further details and explanations of the individual components of the invention follow this initial description. As shown in Fig. 1, in the present invention, separate technology-specific management systems are utilized to manage individual technology domains in the enterprise 110. The example embodiment of Fig. 1 has three technology domains. Technology domain A 102 is managed by management system A 122, technology domain B 104 is managed by management system B 124, and technology domain C 106 is managed by management system C 126.

Technology domains A 102, B 104, and C 106 are comprised of elements that are managed devices, networks, systems, and applications. A managed device is any device that can be modeled in a network management system. The managed devices include not only hardware devices such as personal computers, workstations, hubs, bridges and routers, but also software applications. Domains are constructed in accordance with the particular organizational principle by which elements are grouped in a particular network. In general, network elements may be grouped in any way that serves as an aid in understanding and managing the network. Common grouping principles include grouping with respect to topology, device type, location, managerial domains, and/or the organizational structure of a network enterprise.

The management system components 122, 124, and 126 may be filled by Aprisma Spectrum, Hewlett-Packard (HP) OpenView, or any other compatible management system, device or agent capable of managing the associated technology domain. As discussed in more detail later, the management systems 122, 124, and 126 of the invention may be network management systems, element management systems, enterprise management systems, or any other management devices in any combination suitable for

managing the networks, devices, systems and applications in the associated technology domain.

The comprehensive network management system of the invention is comprised of conceptual layers, with each layer being successively broader in scope and in what it can manage. At the lowest level of the embodiment of the invention depicted in Fig. 1 is the enterprise 110 and technology domains 102, 104, and 106. The intermediate level of this embodiment is an intra-domain management level, where the individual technology domains are managed and various intra-domain management tasks are performed. The highest level is an inter-domain management level, where the intra-domain management systems and levels are themselves managed and various inter-domain management tasks are performed. In alternate embodiments of the invention, there may be multiple intermediate layers, which may be intra-domain management levels that manage individual domains or other intra-domain management levels, or may be inter-domain management levels that manage intra-domain management levels or even other inter-domain management levels.

The basic structure of the present invention is therefore related to what is sometimes called the "divide and conquer" method of network management. A network is partitioned into logical domains where each domain is managed more or less in isolation by low-level management systems. A higher-level management application then presides over the lower-level systems. This higher-level application is sometimes called a manager of managers (MOM). The basic enabling technology for the present invention is therefore the same technology that permits the operation, administration and maintenance (OAM) of the underlying networking technologies.

As shown in Fig. 1, each technology domain A 102, B 104, and C 106 has an associated intra-domain management layer- i.e. domain A 102 is associated with intra-domain management layer A 130, domain B 104 is associated with intra-domain management layer B 150, and domain C 106 is associated with intra-domain management layer C 160. The figure in the text shows a basic two-layer management level system; however, the invention may

have any number of intermediate layers and therefore the scope of the invention includes all two and higher layer systems.

In intra-domain management layer A 130 of Fig. 1, management system A 122 collects data from respective technology domain A 102 and makes it available to intra-domain data collection function 134. This data is then provided to, and utilized by, inter-domain management layer 140 to determine what intra-domain instructions should be sent from intra-domain instruction function A 132 to management system A 122 for implementation in respective technology domain A 102.

Similarly, in intra-domain management layers B 150 and C 160, respective management systems B 124 and C 126 collect data from respective technology domains B 104 and C 106 and make it available to respective intra-domain data collection functions B 154 and C 164. This data is then provided to, and utilized by, inter-domain management layer 140 to determine what intra-domain instructions should be sent from respective intra-domain instruction functions B 152 and C 162 to respective management systems B 124 and C 126 for implementation in respective technology domains B 104 and C 106. All of these functions are typically implemented as one or more software applications, using any convenient and suitable method and/or language known in the art.

Intra-domain management layer A 130 also includes intra-domain event correlation engine A 136, which receives data from management system A 122 on events within domain A 102 and then maps certain of them into alarms and possible actions to be sent back to management system A 122. There is also an intra-domain service level management (SLM) function A 138 that receives service data from management system A 122 that is used to develop service instructions to be sent back to management system A 122 for management of intra-domain services.

Similarly, intra-domain management layers B 150 and C 160 also include respective intra-domain event correlation engines B 156 and C 166 and respective intra-domain service level management (SLM) functions B 158 and

C 168. The purpose and structure of these functions in the present invention are discussed in more detail later. These functions are typically implemented as one or more software applications, using any convenient and suitable method and/or language known in the art. There are several commercially available systems having these functionality, including Aprisma Management Technologies' Spectrum, HP's Openview, Riversoft's, OpenRiver, Tivoli's TME, Computer Associates UniCenter, so-called "home-grown" systems, and others.

Inter-domain management layer 140 is comprised of inter-domain data correlation function 142, inter-domain event correlation function 146, inter-domain service level management function 144 and business process management function 148. Inter-domain data correlation function 142 receives the data collected by management systems A 122, B 124, and C 126 from respective intra-domain data collection functions A 134, B 154, and C 164 and sends instructions to intra-domain instruction functions A 132, B 152, and C 162. The inter-domain data correlation function 162 is typically implemented as a software application, using any convenient and suitable method and/or language known in the art.

Inter-domain event correlation function 146 receives inter-domain event data from inter-domain data correlation function 142 and uses it to map certain of the events into alarms and actions that are sent back to inter-domain data correlation function 142. Inter-domain service level management function 144 receives service data from inter-domain data correlation function 142 and uses it to manage inter-domain services. Business process management function 148 receives service management data from inter-domain service level management function 144 and uses it to determine whether business objectives and policies are being met, as well as for strategic business planning. The purpose and operation of these functions in the present invention are discussed in more detail later. Again, all of these functions are typically implemented as one or more software applications, using any convenient and suitable method

and/or language known in the art and there are several commercially available systems.

It must be noted that the specific devices and systems mentioned herein are examples only, and that alternate constructions, configurations, components, or methods of operation of the invention are to be considered within the scope of the invention. In particular, the network management components may include Aprisma Spectrum, HP OpenView, or any other compatible network, enterprise or other type of management system known in the art. The invention may depend on a network management system or on a collection of element management systems. The former is the preferred embodiment. The communication protocols among management systems may use SNMP, CMIP, CORBA, TL-1 or any other compatible protocols. The communication protocols between management system and managed element may use SNMP, CMIP, CORBA, TL-1 or any other compatible protocols.

The purpose of the comprehensive management system of the invention is to manage all of the types of devices, media, networks, computer systems, software applications, and services that are associated with a technology domain. Examples of the different types of networking technologies that may be part of a technology domain and therefore need to be managed with the invention include, but are not limited to: virtual private networks (VPN), optical networks, Quality-of-Service networks, active programmable networks, wireless networks, ATM switched networks, frame relay networks, cable networks, and customer premises networks (LANs). Different networking technologies may be distinguished with respect to the properties and functionality of transmission devices used, the type of transmission media employed, and the physics and format of data as it travels over the media. Each presents unique management challenges that must be solved in order to achieve comprehensive management.

Fig. 2 is a table summarizing the different dimensions of integrated network management. Networks and their associated systems and services must be viewed at multiple levels of abstraction in order to achieve

comprehensive management. As shown in Fig. 2, on one level are the generic network components 210, such as devices, media, computers, applications, and services. At another management level are network management functions 220, such as fault, configuration, accounting, performance, and security. Still another level treats the network in terms of increasing levels of abstraction 230, starting with the element level, then the network level, the service level, and finally the business management level. At other management levels are service networks 240 and voice/data networks 250.

Fig. 3 is a block diagram illustrating the generic components of a network. As shown in Fig. 3, the network infrastructure is comprised of the transmission devices 330 that receive traffic from, and forward traffic to, other transmission devices. Examples of such devices include, but are not limited to, routers, hubs, switches, and access devices for wireless networks, cable modems, satellite stations, etc. Traffic flows over the transmission media 310 and 320. Examples of transmission media include, but are not limited to, copper wire, coaxial cable, fiber optic cable, telephone lines, and airwaves.

The generic network of Fig. 3 is also comprised of the computer systems 340 that reside on a network, such as desktop computers, workstations, servers, mainframe computers, laptop computers, and even telephony devices, the software applications 350 that run on the computer systems 340, and the various services 360 that are supported by the software applications 350. Examples of software applications include, but are not limited to, document writing applications, database applications, and scientific applications that support mathematical computation and simulations. Also included are distributed applications that span multiple computer systems that may even be distributed over separate networks. Examples of services 360 include, but are not limited to, such things as electronic commerce, inter-continental email, and distance learning.

A virtual private network (VPN) is a good example of a particular type of network that the present invention must manage. A VPN is a network that is constructed by using both public and private media to connect transmission

devices. For example, with reference to Fig. 3, transmission media 310 might include a public network such as the Internet, while transmission media 320 might be a business' private LAN. There are a number of systems that enable the creation of networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. A good example is the VPN service offered by Vitts Networks via their *Protected Service Network.*

One of the underlying technologies that support VPNs is called "IP tunneling." Conceptually, the idea is a private tunnel embedded within transmission media 310 that connects, for example, business-to-business electronic trading. The tunnel should be virtually impenetrable by unauthorized traffic and hackers with malicious intent. The tunnel is physically implemented by a combination of several technologies, including encryption, packet monitoring, firewalls, and network address translation (NAT). The latter technology allows businesses to hide their private IP addresses behind a NAT server so that only the IP address of the NAT server is exposed to the public network.

VPN technology therefore raises several management challenges. One is how issues of quality of service and service guarantees are handled. Since public media are not under the control of service providers, it is difficult to ensure end-to-end application performance when traffic traverses public media. The current solution to this problem is to guarantee a certain quality of service only from customer premises to the edge of the public network. Needless to say, this solution is not entirely acceptable to consumers.

In some VPN configurations, the transmission media and networks are actually owned and operated by separate service providers. This situation presents yet another set of management challenges. With reference to Fig. 3, if there are a number of transmission media 310, each owned by separate service providers, then there are likely to be restrictions on what traffic is allowed to traverse the media. This situation is becoming common in the USA. One

approach to the problem is "policy-based routing." Simply stated, there is a policy database that describes admissible flows of traffic among the edge routers of service provider networks, e.g.: Port x on router A is allowed to forward traffic to port y on router B. As policies are modified to reflect business agreements among service providers, a policy enforcer configures the edge routers accordingly.

Another good example of a particular type of technology that the present invention must manage and that presents unique management challenges is the optical network. Optical networks (a.k.a. photonic networks, or Wavelength Division Multiplexing (WDM) networks) are networks whose transmission devices transmit data in the form of wavelength pulses rather than electronic signals. Optical networks are deployed widely in backbone networks in the USA and Europe for telecommunications applications. The speed of data transmission over a single wavelength is many orders of magnitude faster than electronic signals over fiber or copper. Thus, with single wavelength optical networks, the volume of traffic that can be carried over an optical network is limited only by the processing power of the transmission devices, where processing includes the translation of electronic signals into pulses and vice-versa.

The next evolution in optical networking is dense wavelength division multiplexing (DWDM). The physics of light is such that forty or more wavelengths may be utilized in a single fiber and the transmission devices may still distinguish among them. An increase in available bandwidth by at least forty orders of magnitude is an obvious result. The general consensus is that DWDM will be the technology of choice for networking during the 2000s, through which virtually unlimited bandwidth, at least at the backbone level, will be available. However, the actual volume of traffic that can be carried over an optical network is still going to be limited by the processing power of transmission devices.

Thus, in DWDM optical networks, the first challenge is to manage the new transmission devices in the classic style of element management. For

example, the management system must be able to monitor the performance of each wavelength. It must assist operators in troubleshooting the network by isolating questionable wavelengths and the possible locations of degradation. A second challenge is to provide inter-operability of WDM management agents with other network management systems.

A further management challenge presented by DWDM networks is the challenge of service provisioning. If a service provider wishes to offer optical bandwidth capacity to consumers, an apparatus is required to allocate, maintain, and de-allocate optical channels over the network. A single channel might be adequate to accommodate several small customers, while a large customer might require two or more channels. However, in order to allocate bandwidth intelligently, the service provider will need to know the amount of used and unused capacity per channel. Thus, a management system that can monitor the throughput over a DWDM optical network and infer reasonable measures of used/unused channel capacity is an important requirement.

The present invention also must manage quality of service (QoS)-based networks. A QoS-Based network is typically a traditional-type network that additionally accommodates multiple qualities of service. The classic example is a multi-media network that carries traffic for diverse kinds of applications, where some traffic can withstand latency but other traffic cannot. One example is a QoS-based network currently under development at Cisco Systems, called a Multiprotocol Label Switching (MPLS) network. MPLS and many other QoS-based networks are based on a resource reservation protocol.

MPLS networks are networks whose transmission devices make decisions about forwarding traffic based on the following constraints: (i) topology, (ii) bandwidth requirements, (iii) media requirements, and (iv) packet labeling. MPLS-based networks center around the idea of constraint-based routing, in which the path for a traffic flow is the shortest path that meets a set of known constraints. When packets enter an MPLS-based network, labeling edge routers (LERs) stamp them with a label. The label contains information on the packet source, destination, bandwidth, delay, socket information, and

priority. Once the LER classifies and stamps the packet, it is assigned to a labeled switch path (LSP). As the traffic moves over the assigned LSP, routers place outgoing labels on the packets, again with respect to known constraints.

Some arguments for MPLS-based networks are the following:

- Near-optimal use of backbone bandwidth. Specifically, the best route between a source and destination is determined taking into account the known constraints.
- Reduction in operating costs. With MPLS traffic engineering, an operator does not have to manually configure the network devices to set up explicit routes. The decision-making is automated in the transmission devices.
- Dynamic adaptation and graceful recovery. MPLS-based networks should recover from link or node failures that change the topology of the backbone by adapting to new sets of constraints.
- Regulation of quality of service. From a QoS standpoint, service providers should be able to manage different kinds of data streams based on service priority. For instance, customers who subscribe to a premium service plan should see minimal latency and packet loss, while other customers should expect periodic delays in data transmission.

A challenge for managing MPLS-based networks is to verify service levels agreements (SLAs) made with consumers, where consumers have the option of various service levels. This means that measurable parameters must be found to include in the agreement. Transactional response time is a popular parameter to include in an SLA. However, the guarantee is typically a blanket value, e.g. "a round trip delay of packets sent from the customer site to the edge of the Internet of 50 milliseconds or less." Response time management will be harder with MPLS-based networks, and with QoS-based networks in general. Since there will be multiple grades of services offered to consumers, and assuming that transactional response time continues to be used as a performance measure in SLAs, then there will essentially be multiple response

time guarantees. This clearly will add further complexity to the service providers' management systems.

Further management challenges are presented by the nascent technology known as active networks. Active networks, unlike traditional networks, are not passive carriers of bits but instead provide the capability for the user to inject customized programs into the networks. The network nodes interpret these programs and perform the desired operation on the data flowing through the network. Management challenges presented by active networks include the need for a closer monitoring of the packets and data elements that traverse the network, since networks will now be controlled by the traffic flowing through them rather than the other way around. Configuration management, the management area involving setting up transmission devices, will also need to be treated in a new manner. In particular, note that it is also possible for only part of an end-to-end network to be occupied by an active network, and thus comprehensive management will be required.

The previous discussion has focused on some of the different types of networking technologies that can be managed by the comprehensive network management system of the invention. It is clear that there are also other types of elements between the networking components and the end-user that must be managed including, for example, computers, applications, and video, voice, application and data services. Thus, the management of network services extends beyond management of just the network.

The present invention makes use of integration of element and network management. Fig. 4 illustrates two different conceptual models for this task. The dotted lines in Fig. 4 indicate "managed scope" and the horizontal lines indicate the divisions between the network and service management level 420, the element management level 430, and the element level 440. Block 410 illustrates an element-centric management system. In the element-centric approach, there is a collection of element management systems 450 for managing elements 470. Each element management system 450 passes management information to a higher-level network management system 460. It

can be seen that method 410 includes an intermediary set of element management systems 450 (indicated by black nodes) between the network management system 460 and the "bare" network elements 470. Thus, the network management system 460 is once removed from the bare elements 470. Block 480 illustrates a network-centric management system, in which the network management system 460 communicates directly with the elements 470.

Both approaches are seen in the industry. The latter approach, for example, is taken by Aprisma's Spectrum. There are trade-offs between the two approaches. Spectrum is popular in the industry in part because it provides multi-vendor management from a single management station. This means, however, that Spectrum engineers have to build management modules for new element types as they enter the market, which in turn means that they have to understand the differences between old and new network technologies, the information models of each technology, and the specific management methods required by each technology. This is, of course, feasible, but it is very labor-intensive.

The element-centric approach requires roughly an equal amount of work, but has as a clear disadvantage the common problem of the proliferation of point management solutions, each requiring deployment, configuration, and operational learning curves. A further disadvantage is the lack of a consistent operational interface. What often happens, therefore, is that new technologies are developed in research labs in accordance with the element-centric philosophy, in order to initially develop appropriate management techniques. Once the technology settles, vendors such as Aprisma incorporate the management methods into an existing commercial network management system. It is expected that this approach will frequently be utilized in the addition of new managed elements and systems to the lower-level management systems of the invention. An advantage of the present invention is that these additions will be hidden from the higher, inter-domain levels, vastly reducing the need for such things as operational learning curves.

In the industry, the word "enterprise management" has come to connote the management of applications, systems, and networks. In this respect, an enterprise management system is already a multi-domain management system. Fig. 5 is a block diagram illustrating the conceptual architecture of an enterprise management system that may be employed for cross-domain management in an embodiment of the invention.

In Fig. 5, network management system or systems 510, systems manager or managers 520, and application manager or managers 530 are themselves managed by enterprise management system 500. The various underlying management systems 510, 520 and 530 may be any of the many such management systems known in the art that are capable of being managed by an enterprise management system. Enterprise management system 500 may be the Aprisma Spectrum Enterprise Manager or any other management system known in the art that is capable of managing the various underlying management systems 510, 520, and 530.

Often, management systems 122, 124, and 126 of Fig. 1 will be enterprise management systems. However, not all management systems will have to monitor and control computer systems and applications in addition to the network. For example, the management of an optical network does not include the management of end user systems and applications, although the health of an optical network will affect the health of end user applications. For this reason, management systems 122, 124, and 126 in Fig. 5 may be simple network, application, or systems managers or agents.

While enterprise management and the comprehensive management of the invention share certain elements, there are a number of aspects of comprehensive management that enterprise management cannot provide. By its very definition, enterprise management is not truly comprehensive in nature, being specifically established to provide network, traffic, computer system and application management solely for a single enterprise (i.e. a single business entity). The comprehensive management of the invention is, in many ways, the sum of enterprise management, plus service provider network management for

as many service providers as are part of the system being managed. Further, enterprise management typically does not manage according to the levels in the TMN hierarchy, discussed later with reference to Fig. 9, does not provide Service Level Management, discussed later with reference to Fig. 10, or deal with the interface between the two. In addition, the comprehensive management of the invention includes the management of multiple networking technologies, at the core network, edge network, and customer premises and, in particular, allows the TMN model and service level management to be applied to all these domains. Finally, the comprehensive management of the present invention provides both business level management and a generally higher level of management abstraction, neither of which is available with enterprise management.

Fig. 6 is used to illustrate the manner in which the invention may be used to manage an example network-- a multi-provider VPN. Fig. 1 illustrated how the management systems of the present invention each manage individual networking technology domains. The example embodiment in Fig. 6 shows three such domains: a customer premises network 610, an ATM network 620, and an optical backbone 614. In this embodiment, the individual elements in each of domains 610, 612, and 614 are managed by appropriate device managers 620. The device managers 620 within each domain are themselves managed by a domain-specific network management system 630.

In this example, each network is provided and operated by a third party utilizing its own management platforms and management processes. If there is a VPN that spans across all of those networks, then clearly the management of the VPN depends upon management information collected by the respective domain network management systems 620. Thus, Fig. 1 shows *intra*-domain data from domains A 102, B 104, and C 106 being passed to an *inter*-domain data correlation function 142. The inter-domain data correlation function 142 processes intra-domain data and returns data back to domains A 102, B 104, and/or C 106 in the form of operational instructions. Such operational instructions may have to do with faults, configurations, or service provisioning

In fact, large businesses often have to construct VPNs that span across multiple heterogeneous networks, where some of the networks are privately owned. This "separation challenge" is illustrated in Fig. 7. Fig. 7 is a conceptual depiction of a such a network, having managed domains controlled by different entities. In Fig. 7, domain *X* 720 is managed by provider *A* 730, but a service *S* 710 offered by *A* depends upon a domain *Y* 740 that is managed by provider *B* 750. As mentioned, this separation challenge is common in the industry. The result of such a situation, from the network operator's point of view, is management complexity in terms of security management, operations management, problem management, configuration management, policy management, change management. The present invention is specifically designed to reduce or eliminate these problems.

There are four logical approaches to the problem presented by the example of Fig. 7:

1. *A* limits its service offerings to those that depend upon the networks under its control.
2. *A* doesn't offer service guarantees in cases where the service depends upon networks not under its control.
3. *A* and *B* enter an arrangement whereby network operators collaborate to handle service degradations and faults.
4. *B* opens its domain to *A*'s management system, or vice versa.

As can be seen, approaches 1 and 2 sidestep the separation problem altogether, while approaches 3 and 4 tackle it head on. In particular, approach 4 returns directly to the need for the integrated management provided by the comprehensive network management system of the invention.

Another common manifestation of the separation problem is seen even within businesses that control their own local services, where, for example, *A* is a staff dedicated to network management (domain *X*) and *B* is a staff dedicated to systems and applications management (domain *Y*). Often it seems that these people rarely talk to each other, and when they do, it takes the form

of finger-pointing. Clearly, an integrated management system would also help to alleviate this internal separation problem.

The preferred embodiment of the invention employs domain-specific event correlation. Event correlation entails observing cause-and-effect relations between certain events, inferring an alarm from a set of related events, and/or identifying the "culprit" event in a "misbehaving" enterprise. In practice, a particular network management system will collect numerous events and statistics as it monitors the elements in its respective domain. The task of event correlation is to map certain collections of events scattered in space and time into *alarms* and possible *actions*. There are several paradigms in the industry for event correlation, including rule-based reasoning, model-based reasoning, state transition graphs, codebooks, and case-based reasoning. Additional paradigms are also currently being investigated in research laboratories, e.g. fuzzy logic and neural networks.

Fig. 8 depicts intra-domain event correlation as utilized by the present invention. As shown in Fig. 8, domain 810 is subject to event monitoring 820. When events occur, they are processed by the event correlation engine 830 and mapped into alarms and actions 840. Any of the paradigms for event correlation mentioned previously would be suitable. Many commercial management systems, including Spectrum, now either have event correlation engines or are integrable with them.

Regardless of the particular paradigm used, domain-specific event correlation is another example of the "divide and conquer" approach to network management that is employed by the present invention. In general, single event correlation engine for a large heterogeneous networking system will not scale. Thus, it is advisable to employ separate correlation engines for each individual domain, where the output of each engine is passed to a higher-level correlation engine. The inter-domain data correlation function 146 of Fig. 1 is such a higher-level correlation engine. In this capacity, its domain, i.e. its input, is the space of intra-domain alarms.

The invention therefore requires correlation engines for both lower-level intra-domain management systems and for higher-level inter-domain management systems. The idea is similar to the concept of a manager of managers (MOM). There are in fact several commercial products available that act as MOMs. Their sole function is to receive input data from lower-level network or element management systems, process the data, and output data in the form of reports and recommended actions.

The additional consideration of systems and application management ties in with the need for domain-specific event correlation. A common question regarding an end user's complaint is "Is it a network, systems, or application problem?" A response time management (RTM) system, for example, can raise a problem regarding sluggishness in application transactions, but further work needs to be done in order to determine whether the cause of the problem has to do with the application, the computer system on which the application resides, or the network. An event correlation system that covers systems and application events helps in isolating the root cause of the problem.

An important concept in network management is the five-layer Telecommunications Management Network (TMN) model shown in Fig. 9. The TMN model is partitioned into five layers: the element layer 910, the element management layer 920, the network or enterprise management layer 930, the service management layer 940, and the business management layer 950. Each layer, going from bottom to top, represents a transformation from technical detail towards more business-oriented information.

The business layer 950 is concerned with the overall management of the business. As such, it covers aspects relating to business processes and strategic business planning. Further, it seeks to capture information that may be used to determine whether business objectives and policies are being met. The service management layer 940 is concerned with the management of services provided by a service provider to a customer or to another service provider. Examples of such services include billing, order processing, and trouble ticket handling. The enterprise/network management layer 930 is concerned with a network with

multiple elements. As such, it supports network monitoring and remote configuration. In addition, this layer supports issues such as bandwidth control, performance, quality of service, end-to-end flow control, and network congestion control. The element management layer 920 is concerned with the management of individual network elements including, for example, switches, routers, bridges, and transmission facilities. The element layer 910 refers to the bare elements that are to be managed.

The TMN idea has influenced those businesses that own their own networks as well as businesses that outsource pieces of the network operation to service providers. For the most part, commercial networks are manageable up to, and including, the network layer. The ideas of "services" and "service level agreements" are now on the minds of business executives and service providers.

A service may be viewed from a user's point of view, from a business' point of view, or from the network's point of view. The service provided by an optical network, for example, is the allocation of bandwidth to a customer. This service from a business' point of view may be decomposed into the service provided by the optical network plus the services provided by its own local network, systems, and applications. This is therefore yet another example of the divide and conquer technique, whereby a higher-level service is comprised of several lower-level services. Thus, with reference to Fig. 1, end-to-end services are managed at inter-domain level 140, and local services are managed at the intra-domain levels 130, 150 and 160.

Fig. 10 is a conceptual depiction of how service level management is therefore utilized in conjunction with enterprise management in an embodiment of the invention. In Fig. 10, network management system or systems 1040, systems manager or managers 1030, and application manager or managers 1020 are themselves managed by enterprise management system 1010. In turn, enterprise manager 1010 is subject to service level management 1050. As previously discussed, service level management 1050 is concerned with the management of services provided by a service provider to a customer or

another service provider. As in Fig. 5, the network management layer may possibly include the management of computer systems and software applications that reside on the network, and the term "element" is used to include individual systems and applications in addition to transmission devices.

As mentioned previously, the invention provides classical FCAPS management (fault, configuration, accounting, performance, and security management). *Fault management* includes trouble management, which manages corrective actions for service, fault recovery, and proactive maintenance and provides capabilities for self-healing. Trouble management correlates alarms to services and resources, initiates tests, performs diagnostics to isolate faults to a replaceable component, triggers service restoral, and performs activities necessary to repair the diagnosed fault. Proactive maintenance responds to near-fault conditions that degrade system reliability and may eventually result in an impact on services. It performs routine maintenance activities on a scheduled basis and initiates tests to detect or correct problems before service troubles are reported.

Configuration management includes timely deployment of resources to satisfy the expected service demands, and the assignment of services and features to end-users. It identifies, exercises control over, collects data from, and provides data to the network for the purpose of preparing for, initializing, starting, and providing for the operation and termination of services. It deals with logical, service, or custom networks such as the toll network, local public switched telephone network, and private networks. *Accounting management* processes and manipulates service and resource utilization records and generates customer billing reports for services rendered. It establishes charges and identifies costs for the use of services and resources in the network.

Performance management addresses processes that ensure the most efficient utilization of network resources and their ability to meet user service-level objectives. It evaluates and reports on the behavior of network resources and ensures the peak performance and delivery of each voice, data, or video service. *Security management* controls access to, and protects, both the

network and network management systems against intentional or accidental abuse, unauthorized access, and communication loss. Flexibility methods are built into security mechanisms in order to accommodate ranges and inquiry privileges that result from the variety of access modes utilized by operations systems, service provider groups, and customers.

Multi-wave optical networks can be used as an example to illustrate how the TMN model and FCAPS management are applied to a new technology in order that it can be managed with the comprehensive network management system of the invention. As previously mentioned, multi-wave optical networks promise to change the face of communications by enabling advanced applications in federal, scientific, and commercial sectors. The first problem in managing multi-wave optical networks, however, is to develop what is sometimes called an "information model" for the new networking technology, i.e. a model that depicts the physics of optical networks in terms of management concepts. For example, the information model of multi-wave optical networks includes models of optical components (optical-to-electronic terminating equipment, multiplexing equipment, optical amplifiers, etc.) and models of wavelengths (e.g. section trails, multiplex trails, and channel trails). Typically, the information model is used also as a base to develop FCAPS-style and TMN-style management methods for the technology.

Consider what a commercial network management vendor has to worry about in this kind of situation: The vendor is not in the business of developing optical networks. It is in the business of managing them. However, in order to understand how to manage them, the vendor's scientists and architects have to keep close watch on the development of the technology, its special management methods, and its commercial viability.

Aprisma Management Technologies is an example of such a vendor. Aprisma's *Spectrum* is commercially popular; it is good at managing existing enterprise networks, service provider networks, ATM and frame relay networks, cable networks, and others. It is also good at multi-vendor device management and event correlation over single- and multi-domain networks.

Aprisma's stated goal is to provide a comprehensive management solution and, in that regard, it competes with vendors such as HP, Tivoli, Computer Associates, Objective Systems, and a number of start-up companies in the network management space.

The Spectrum system is based on the object-oriented information paradigm, whereby network components are conceived as objects that represent their real-world counterparts. An object-oriented system helps to alleviate the problem of introducing models of multi-vendor elements into an existing system. Further, it expedites the generation of management methods for domains other than networks and network elements. Systems, applications, and service management products are incorporated into Spectrum by third-party vendors.

The object-oriented paradigm is more or less a *de facto* paradigm for developing information models for new networking technologies, including multi-wave optical networks. Since Spectrum's information model is based on the object-oriented paradigm, there is a fortunate commensurability between it and the information models of new networking technologies. It is hard, however, to predict how the information models developed by different networking vendors or vendor consortia will stabilize into a standard, even though they are based on the object-oriented paradigm.

A need in the industry as a whole is to develop a common language for specifying network technologies and the management of them. This, in fact, is the main goal of standards bodies. A good start in that direction is the ITU-T Recommendation G.805 – *Generic Network Information Model* (1995). Many of the management concepts for optical networks, for example, are derived from that document. It is therefore advisable that frameworks for network management systems migrate towards an alignment with such information models. In the preferred embodiment of the invention, this approach is followed.

As previously seen, today's business and service networks are complex. The current state of any particular network has more than likely evolved in a

piecemeal fashion, and thus it will include heterogeneous kinds of network technologies, equipment from multiple vendors, and various kinds of management methods. To make matters worse, management methods vary between countries and even between districts within countries. In many cases, the result is either piecemeal management, in which narrowly focused management solutions co-exist but do not cooperate, or no management at all. The solution is integrated management, in which these management techniques cooperate in a standardized management framework. Thus, the ultimate goal of international standards bodies is to provide a uniform framework and methodology in order to correct the current situation. The problem, however, is that the standardization process is often slow and sometimes doesn't mature into a globally accepted standard.

The goal of a generic framework by which to manage diverse networking technologies is certainly a good idea. However, no matter how much a vendor wants to develop a comprehensive, single-console management system, there will still be times when an integration with another vendor's management system makes good sense. A good example is the integration of an existing management system with a legacy management system.

Further, there is a valid argument that no one vendor can provide all the solutions. As a practical matter, vendors tend to be more or less specialists in one domain or another. For example, some are good at building network management systems, some are good at building network simulation systems, some are good at building trouble ticket and help desk systems, etc. Thus, a direction for future work is to catalogue various kinds of integration patterns and mechanisms by which to implement them.

A high-level operational flowchart of comprehensive network management according to one aspect of the invention is shown in Fig. 11. In Fig. 11, the functional steps starting at box 1110 are carried out simultaneously at all the levels of abstraction of the invention. In other words, the same steps are carried out from the business perspective 1112, the service perspective 1114, the inter-domain perspective 1116, and the intra-domain perspective

1118. All that varies is the level of abstraction upon which the steps operate and the corresponding level of abstraction of the input data and output instructions.

As shown in Fig. 11, data is collected 1130 at a particular level of abstraction by use of an appropriate data collection function. The data is then interpreted 1140 from the appropriate level of abstraction perspective. The manner of interpreting data may be carried out by any of the many means known in the art, including, but not limited to, look-up tables, expert systems, machine learning systems, etc. If the data interpretation 1140 determines that instructions are required for submanagers at a lower level of abstraction 11150, an instruction function at the appropriate level of abstraction sends the required instructions 1160 to the appropriate submanagers.

For example, with reference also to Fig. 1, data from domains A 102, B 104, and C 106 is collected 1130 by intra-domain data collection functions A 134, B 154 and C 164 at the intra-domain level 1118 (130, 150, 160) and provided to the inter-domain level 1116 (140) where it is processed by the inter-domain data correlation function 142. Inter-domain data correlation function 142 may also provide this data to inter-domain event correlation function 146. If data correlation function 142 determines, either from its own analysis or based on feedback from inter-domain event correlation function 146, that instructions to management systems A 122, B 124 and/or C 126 are required 1150, then inter-domain data correlation function 142 provides instructions to one or more of intra-domain instructions functions A 132, B 152, and C 162 at the intra-domain level 1118 (130, 150, 160). Intra-domain instructions functions A 132, B 152, and C 162 then provide appropriate instructions to respective management systems A 122, B 124 and C 126 at the intra-domain level 1118 (130, 150, 160). From this example, it is to be understood that the actions of the invention at the other levels of abstraction would have a similar character, according to the principles around which that level of abstraction is organized.

The following steps are development steps by which the current invention may be constructed for each individual technology domain.

1. Element development
2. Element-style management
3. Fault and Configuration Management in Element-style Management
4. Network-style management
5. Intra-domain event correlation
6. Intra-domain service level management
7. Inter-domain network management
8. Inter-domain event correlation
9. Inter-domain service level management
10. Inter-domain business process management

It is to be understood that these steps apply to the implementation of management of a single domain, and that similar development steps would therefore need to be applied to each technology domain in order to fully realize the comprehensive network management system of the invention.

What has been described herein is merely illustrative of the application of the principles of the present invention. Other arrangements, methods, modifications and substitutions by one of ordinary skill in the art are also considered to be within the scope of the present invention, which is not to be limited except by the claims that follow.

CLAIMS

What is claimed is:

1. An apparatus for management of a multi-domain communications network comprising, in combination:

at least one inter-domain management layer; and

at least one intra-domain management layer, associated with at least one inter-domain management layer and at least one technology domain or at least one other intra-domain management layer, for managing said associated technology domain or other intra-domain management layer, providing data to said inter-domain management layer, and receiving instructions from said inter-domain management layer.

2. The apparatus of claim 1, further comprising at least one event correlation engine.

3. The apparatus of claim 2, wherein there is a separate event correlation engine respectively associated with each intra-domain management layer and each inter-domain management layer.

4. The apparatus of claim 1, further comprising at least one service level management application.

5. The apparatus of claim 4, wherein there is a separate service level management application respectively associated with each intra-domain management layer and each inter-domain management layer.

6. The apparatus of claim 2, further comprising at least one service level management application.

7. The apparatus of claim 6, wherein there is a separate service level management application respectively associated with each intra-domain management layer and each inter-domain management layer.

8. The apparatus of claim 3, further comprising at least one service level management application.

9. The apparatus of claim 8, wherein there is a separate service level management application respectively associated with each intra-domain management layer and each inter-domain management layer.

10. The apparatus of claim 4, further comprising at least one business process management application.

11. The apparatus of claim 7, wherein there is a separate business process management application associated with each inter-domain management layer.

12. The apparatus of claim 9, wherein there is a separate business process management application associated with each inter-domain management layer.

12. The apparatus of claim 9, wherein there is a separate business process management application associated with each inter-domain management layer.

13. An apparatus for management of a multi-domain communications network comprising, in combination:

at least one inter-domain management layer;

at least one intra-domain management layer, associated with said inter-domain technology layer and with at least one technology domain or at least one other intra-domain management layer, for managing said associated technology domain or other intra-domain management layer, providing data to

said inter-domain management layer, and receiving instructions from said inter-domain management layer;

a respective intra-domain event correlation engine, associated with each intra-domain management layer, for processing intra-domain events and providing alarms and possible actions;

a respective inter-domain event correlation engine, associated with each inter-domain management layer, for processing inter-domain events and providing alarms and possible actions;

a respective intra-domain service level management application, associated with each intra-domain management layer, for receiving service data and developing service instructions for managing services in said associated technology domain or intra-domain management layer; and

a respective inter-domain service level management application, associated with each inter-domain management layer, for receiving service data from at least one associated intra-domain management layer and developing service instructions for managing services in said associated intra-domain management layer.

14. The apparatus of claim 14, further including a business process management application, associated with the inter-domain service level management application of each inter-domain management layer, for receiving service management data from said associated inter-domain service level management function for use in at least one business planning or monitoring function.

15. A method for management of a multi-domain communications network comprising, in combination, the steps of:

managing at least one technology domain or intra-domain management layer with an associated intra-domain management layer; and

managing each associated intra-domain management layer with an associated inter-domain management layer.

16. The method of claim 15, wherein said step of managing each associated intra-domain management layer comprises, in combination, the steps of:

providing data from said associated intra-domain management layer to said inter-domain management layer; and

receiving instructions at said associated intra-domain management layer from said inter-domain management layer.

17. The method of claim 16, further comprising the steps, in combination, of:

performing intra-domain event correlation; and

sending at least one of alarms, data, and instructions to at least one associated technology domain or associated intra-domain management layer based on said event correlation.

18. The method of claim 16, further comprising the steps, in combination, of:

performing inter-domain event correlation; and

sending at least one of alarms, data, and instructions to at least one associated intra-domain management layer based on said event correlation.

19. The method of claim 17, further comprising the steps, in combination, of:

performing inter-domain event correlation; and

sending at least one of alarms, data, and instructions to at least one associated intra-domain management layer based on said event correlation.

20. The method of claim 16, further comprising the steps, in combination, of:

performing intra-domain service level management; and

developing service instructions for managing services in at least one associated technology domain or intra-domain management layer based on said service level management.

21. The method of claim 17, further comprising the steps, in combination, of:

performing intra-domain service level management; and

developing service instructions for managing services in at least one associated technology domain or intra-domain management layer based on said service level management

22. The method of claim 19, further comprising the steps, in combination, of:

performing intra-domain service level management; and

developing service instructions for managing services in at least one associated technology domain or intra-domain management layer based on said service level management.

23. The method of claim 16, further comprising the steps, in combination, of:

performing inter-domain service level management; and

developing service instructions for managing services in at least one associated intra-domain management layer based on said service level management.

24. The method of claim 18, further comprising the steps, in combination, of:

performing inter-domain service level management; and

developing service instructions for managing services in at least one associated intra-domain management layer based on said service level management.

25. The method of claim 19, further comprising the steps, in combination, of:

performing inter-domain service level management; and

developing service instructions for managing services in at least one associated intra-domain management layer based on said service level management.

26. The method of claim 22, further comprising the steps, in combination, of:

performing inter-domain service level management; and

developing service instructions for managing services in at least one associated intra-domain management layer based on said service level management.

27. The method of claim 23, further comprising the step of utilizing service management data from said service level management to perform inter-domain business process management.

28. The method of claim 26, further comprising the step of utilizing service management data from said service level management to perform inter-domain business process management.

29. A method for management of a multi-domain communications network comprising, in combination, the steps of:

managing at least one technology domain or intra-domain management layer with an associated intra-domain management layer;

managing each associated intra-domain management layer with an associated inter-domain management layer;

collecting data from said technology domains and intra-domain management layers;

interpreting said collected data within an appropriate management level of abstraction to determine if instructions are needed at one or more of said associated technology domains and intra-domain management layers; and

sending said instructions to one or more of said associated technology domains and intra-domain management layers when required.

30. The method of claim 29, wherein said step of interpreting includes at least event correlation.

31. The method of claim 29, wherein said step of interpreting includes at least service level management.

32. The method of claim 31, wherein said step of interpreting includes at least business process management.

33. The method of claim 30, wherein said step of interpreting includes at least service level management.

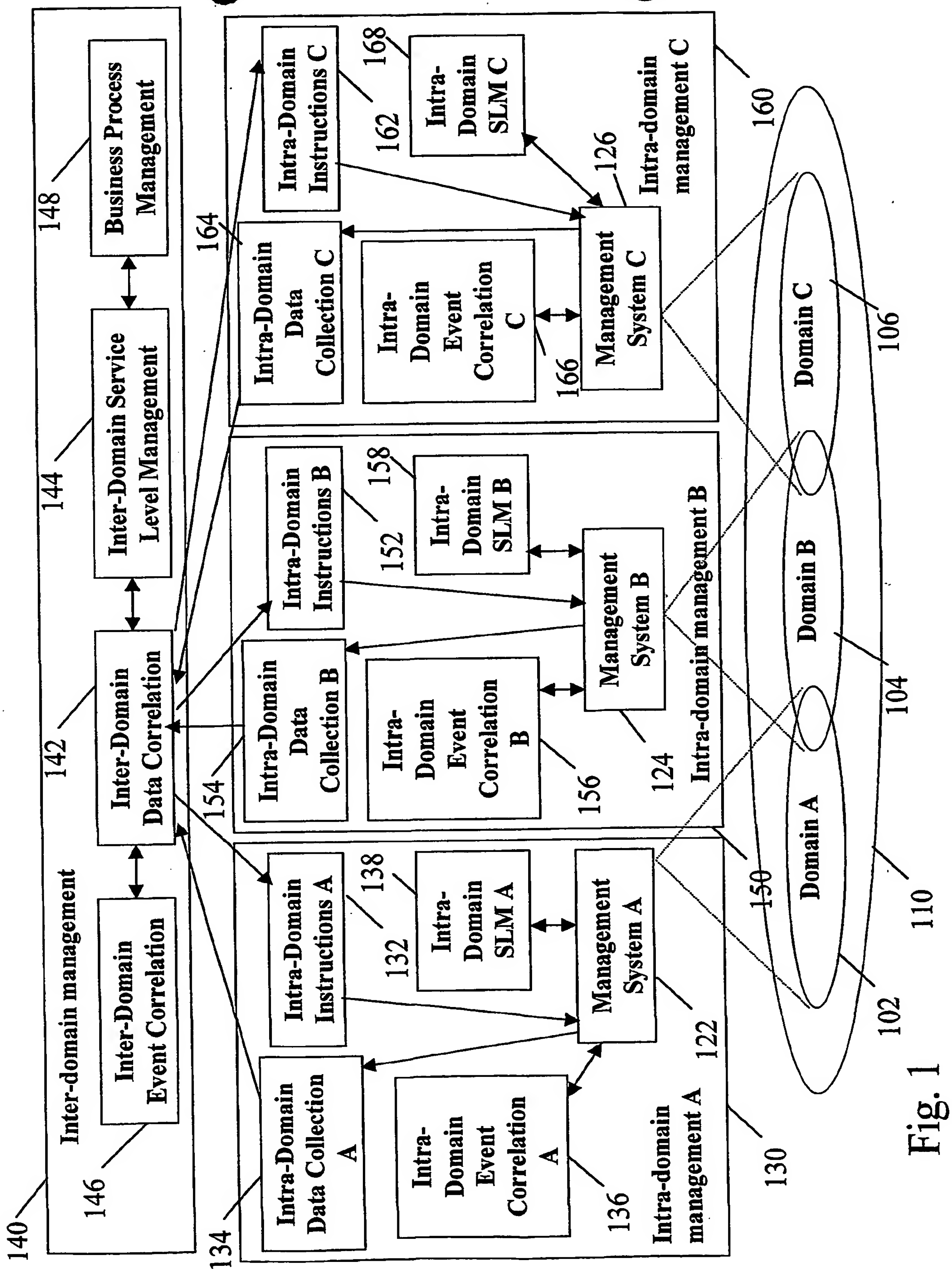

Inter-domain management
Business Process Management
Inter-Domain Service Level Management
Inter-Domain Data Correlation
Inter-Domain Event Correlation
Intra-Domain Data Collection A
Intra-Domain Event Correlation A
Intra-Domain Instructions A
Intra-Domain SLM A
Management System A
Intra-domain management A
Intra-Domain Data Collection B
Intra-Domain Event Correlation B
Intra-Domain Instructions B
Intra-Domain SLM B
Management System B
Intra-domain management B
Intra-Domain Data Collection C
Intra-Domain Event Correlation C
Intra-Domain Instructions C
Intra-Domain SLM C
Management System C
Intra-domain management C
Domain A
Domain B
Domain C
102
104
106
110
122
124
126
130
132
134
136
138
140
142
144
146
148
150
152
154
156
158
160
162
164
166
168

Fig. 1

210	Generic components	devices, media, computers, applications, services
220	Functional areas	fault, configuration, accounting, performance, security
230	Layers of abstraction	element, network, service, business management
240	Service networks	network 1, network 2, … , network n
250	Voice/data networks	network 1, network 2, … , network n

Fig. 2

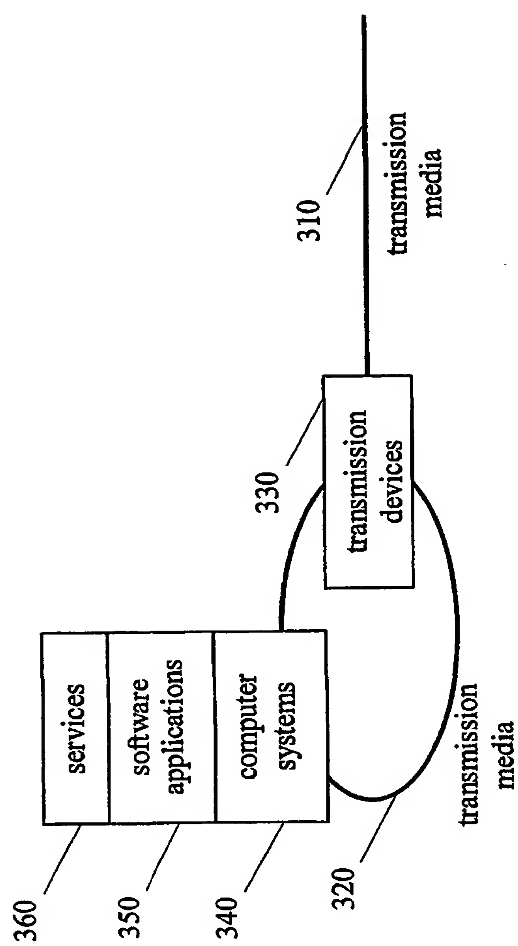

310
transmission media
330
transmission devices
services
software applications
computer systems
transmission media
360
350
340
320

Fig. 3

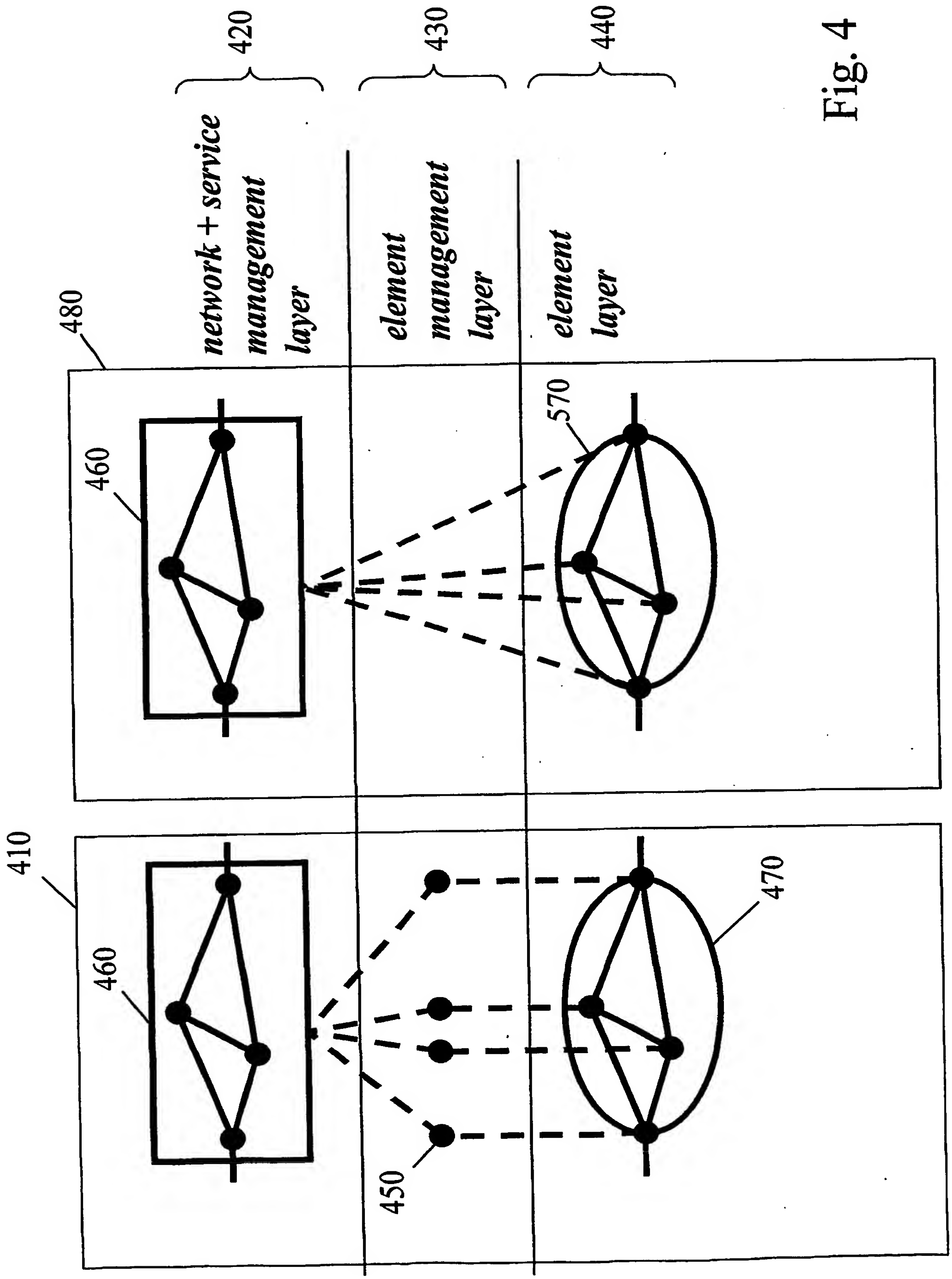

420
430
440
network + service management layer
element management layer
element layer
480
460
570
410
460
470
450

Fig. 4

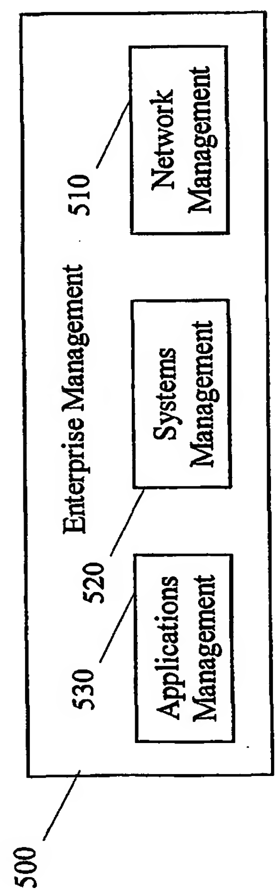

500
Enterprise Management
510
Network Management
520
Systems Management
530
Applications Management

Fig. 5

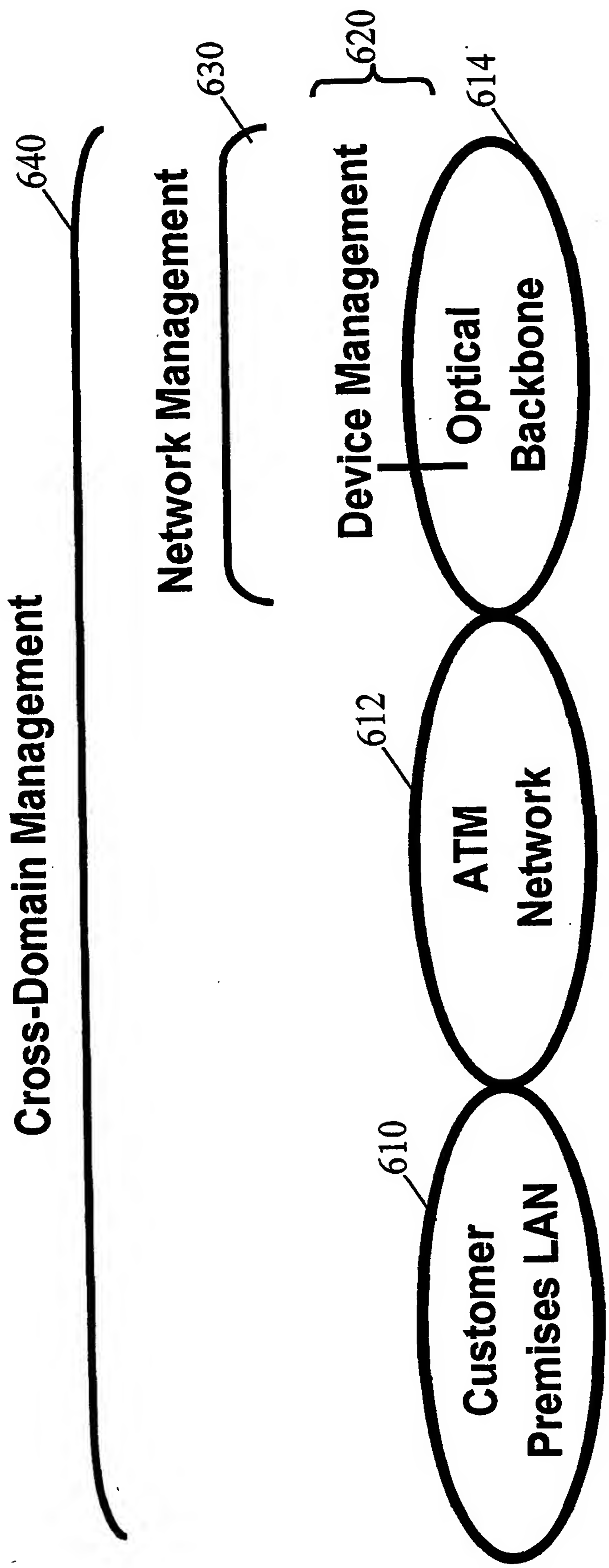

Cross-Domain Management
640
Network Management
630
Device Management
620
614
Optical Backbone
612
ATM Network
610
Customer Premises LAN

Fig. 6

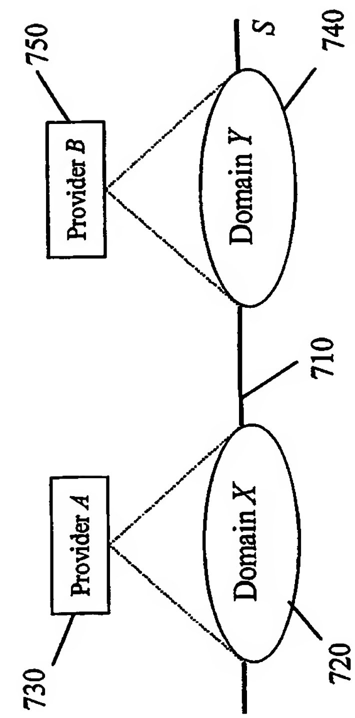
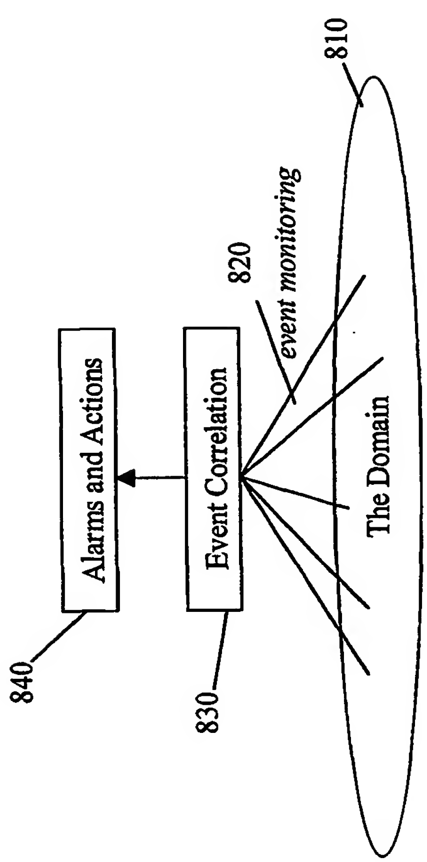


Fig. 7



Alarms and Actions
Event Correlation
event monitoring
The Domain
810
820
830
840

Fig. 8

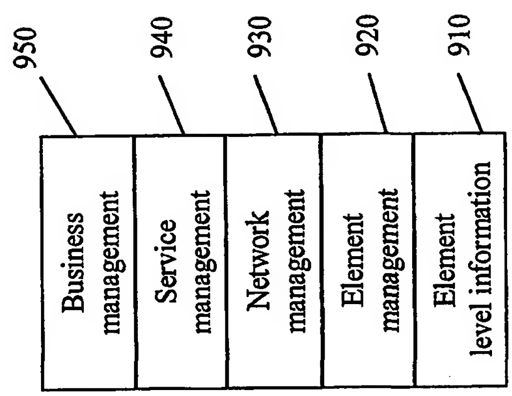

950
940
930
920
910
Business management
Service management
Network management
Element management
Element level information

Fig. 9

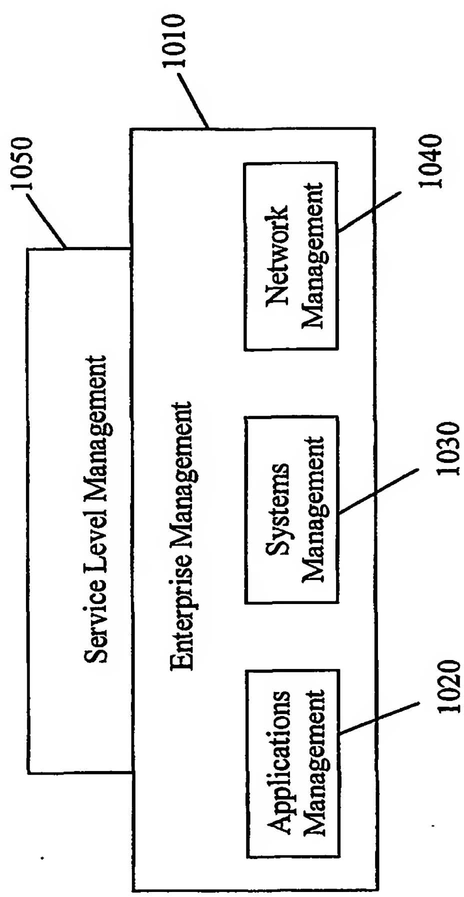

1010
1050
Service Level Management
Enterprise Management
Network Management
1040
Systems Management
1030
Applications Management
1020

Fig. 10

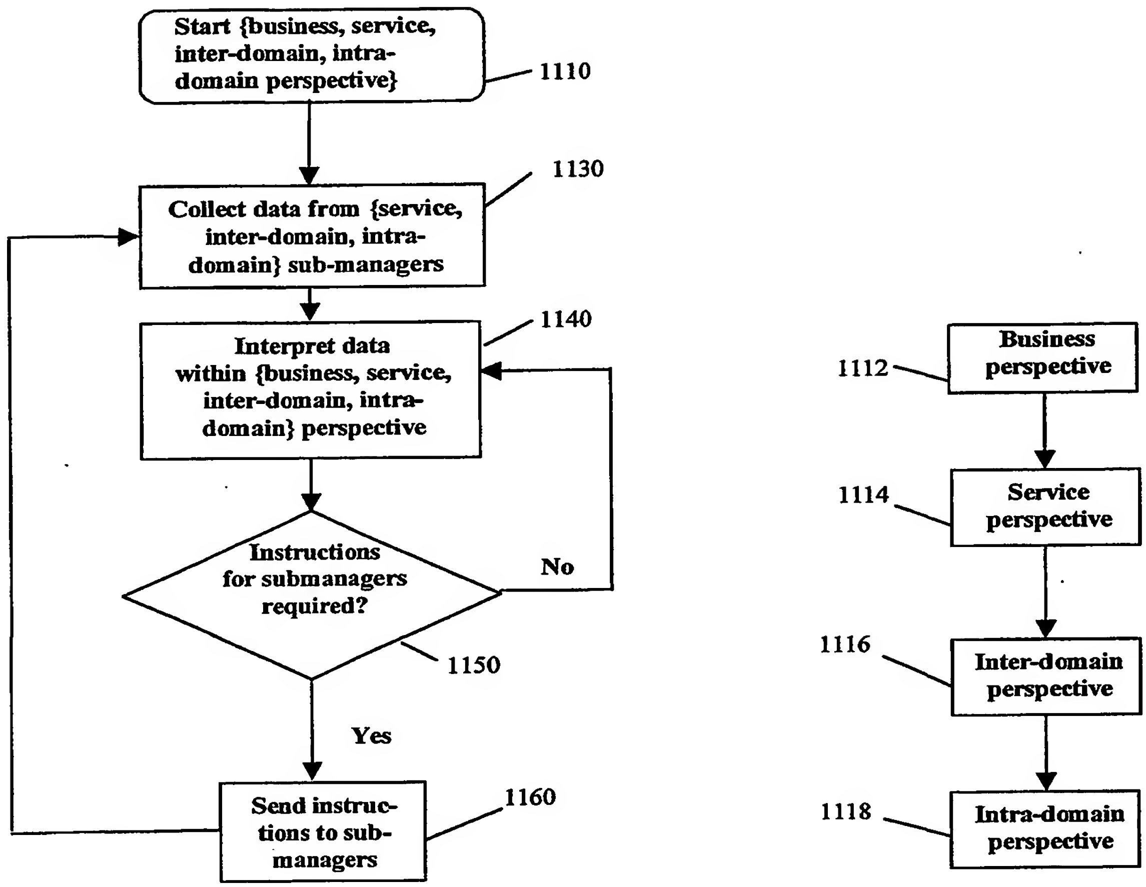

Start {business, service, inter-domain, intra-domain perspective}
1110
Collect data from {service, inter-domain, intra-domain} sub-managers
1130
Interpret data within {business, service, inter-domain, intra-domain} perspective
1140
Instructions for submanagers required?
No
1150
Yes
Send instructions to sub-managers
1160
Business perspective
1112
Service perspective
1114
Inter-domain perspective
1116
Intra-domain perspective
1118

Fig. 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/22107

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 15/173
US CL : 709/224, 226
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 709/224, 226, 249; 370/321, 323; 714/47,48

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

IEEE ONLINE
search terms: QOS, mutli-domains, system or network management, inter-domain

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	SEITZ A Modelling Techique for Inter-Domain Management, IEEE, June 2000, pages 858-862, especially pages 859-861	1-31
A	LEE Design and Implementation of a Configuration Management System, IEEE 1993 pages 1563-1567	1,13,29
A	LEWIS et al., The Development of Integrated Inter and Intra Domain Management Services IEEE May 1999, pages 279-292,	1-31
A	CHUAH et al., QoS Providioning Using a Clearing House Architecture IEEE, June 2000, pages 115-124, especially pages	1 ,13,29
Y	US 5,768,501 A (LEWIS) 16 June 1998, figures 3-10, col. 7, line 56-col. 13, line 53	1-31

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:	
"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E" earlier document published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 AUGUST 2001	11 OCT 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer LARRY DONAGHUE James R. Matthews Telephone No. (703) 305-9675